

Release Notes

IPS Engine 7.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



TABLE OF CONTENTS

Change log	4
Introduction	5
Product integration and support	6
Resolved issues	7
Known issues	9

Change log

Date	Change Description
2021-11-03	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 7.0 build 044.

- [Product integration and support on page 6](#)
- [Resolved issues on page 7](#)
- [Known issues on page 9](#)

IPS Engine 7.0 build 044 is a release to FortiGuard. It is not a built-in release for FortiOS.

For additional FortiOS documentation, see the [Fortinet Document Library](#).

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	7.0
---------	-----

Resolved issues

The resolved issues listed do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
645848	FortiOS provides self-signed CA certificate intermittently with flow-based SSL certificate inspection.
654356	Under next generation firewall (NGFW) policy mode, sessions are not revalidated when security policies change. Workaround: clear the session after a policy change.
672994	Web Filter warning message does not contain certification chain.
673117	Trivial File Transfer Protocol (TFTP) traffic does not work well when TFTP application is set in security policy.
678890	IPS engine stalls. Alarm clock crashes at <code>pat_search_nocase</code> .
681611	IPS engine crashes with <code>ips_dlp_alert</code> .
687885	Inconsistent system performance with RFC2544 IXIA breaking point testing.
691338	Download drops to 0 kbps and slow website access after firmware upgrade.
696619	FortiGate Session Life Support Protocol (FGSP)-synced UDP sessions may be blocked in NGFW policy mode when using asymmetric routing due to policy matching failure. Other traffic types, such as TCP, may be affected in the case of failover of the reply-direction traffic to a different FortiGate in the FGSP cluster.
707907	IPS Engine in deep inspection flow mode does not decrypt some TLS 1.3 sessions, causing problems with application control detection.
709968	FortiGate drops UDP port 5440 traffic after rebooting both FortiGates.
712352	Firewall goes into conserve mode and IPS consumes high memory.
713068	FGSP support in NGFW policy mode.
715136	High memory usage for some slab objects.
718452	<code>set https-replacemsg disable</code> causes connection reset on URLs in URL filter list in flow inspection mode.
719007	URL filtering followed by <code>/*</code> causes rating error.
719252	IPS engine crash.
720605	URL filter with exemptions may not avoid antivirus and IPS inspection.
720943	UTM does not work when the GRE session is created by a specific direction.

Bug ID	Description
721410	fb.watch website cannot open in flow mode plus SSL deep inspection with application control.
721435	Download breaks when the policy is in flow base mode with deep inspection and the NCP application is used on the host
721462	Memory usage increases to conserve mode after IPS Engine upgrade.
724400	facebook.com website gives error in Firefox v89 with flow mode plus deep inspection.
724767	Event log garbles hostname, as HTTP.Suspicious.Headers.With.Special.Characters indicates.
728492	Unable to load instagram.com from Chrome browser without changing TLS Post-Quantum Confidentiality flag from default to enabled.
729249	Web Filter categorizes private IP address/local URLs as newly observed domain.
730137	Unable to access website when the policy is in flow based with Web Filter enabled.
731459	In NGFW policy mode, disabling security policy does not stop current traffic passing the firewall.
735893	After Chrome 92 update, FortiOS 6.2, 6.4, and 7.0 cannot reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.
736906	The default <code>np-accel-mode basic</code> causes sporadic HTTPS deep inspection transaction failures with Application Control.
738144	The UTM function only works for a few seconds in GRE session.
741643	Traffic may be incorrectly blocked or matched with the wrong security policy in NGFW policy mode.
744352	Some websites open very slow in flow mode plus SSL deep inspection.
744888	FortiGate drops SERVER HELLO when accessing website using flow based policy with deep SSL inspection.
745163	Website ad.doubleclick.net cannot open in flow mode with deep packet inspection and a security profile in Chrome.

Known issues

There are no known issues with this release of IPS engine version 7.0 for FortiOS.

To report a bug, please contact [Customer Service & Support](#).



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.